Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 16 January 2004

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
www.whitehouse.gov/homeland

Daily Overview

- IDG News Service reports that after releasing a new version of the Mimail e−mail worm last week, virus authors are using a new tool to help it spread −− spam e−mail containing a Trojan horse program that, once installed, retrieves and installs the worm which targets customers of EBay's PayPal online payment service. (See item 6)

- The Associated Press reports that according to the results of a federal study, the current flu vaccine has had little effectiveness against preventing flu−like illnesses, from the common cold to strep throat. (See item 20)

- Global Security Newswire reports with the threat of terrorism looming over this year's Summer Olympics in Athens, the United States is helping Greece to deploy radiation detectors in a bid to prevent a radiological attack on the summer games. (See item 25)

DHS/IAIP Update *Fast Jump*

Production Industries: **Energy**; **Chemical**; **Defense Industrial Base**

Service Industries: **Banking and Finance**; **Transportation**; **Postal and Shipping**

Sustenance and Health: **Agriculture**; **Food**; **Water**; **Public Health**

Federal and State: **Government**; **Emergency Services**

IT and Cyber: **Information and Telecommunications**; **Internet Alert Dashboard**

Other: **General**; **DHS/IAIP Web Information**

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *January 15, Washington Business Journal* — **Cold snap pushes natural gas demand to record high. It's been so cold in the Washington area this month, that utility Washington Gas says it set a one−day record Saturday, January 10. On that day, the company says it delivered 1.45 billion square feet of natural gas to customers, beating last year's record 1.4**

billion square feet set on January 3, 2003. That is the equivalent of about 14.5 million "therms," the unit of measurement commonly used in the natural−gas industry. Washington Gas says on a typical January day its customers use about 9 million therms of natural gas. **The company assures that despite the higher−than−normal demand, it has reserves to meet requirements.** In October, Washington Gas had predicted area heating customers would pay about 15 percent less than a year ago. It based that estimate on forecasts for a milder−than−normal winter. Despite the weeklong cold spell, that may still hold true. Temperatures during last year's six−month winter heating season were about 16 percent colder than normal.
Source: http://washington.bizjournals.com/washington/stories/2004/01 /12/daily34.html

2. *January 15, Department of Transportation* — **Maritime Administration approves deepwater liquid natural gas port. The U.S. Maritime Administration approved on Thursday, January 15, a new deepwater liquid natural gas (LNG) port. The LNG port, to be built by El Paso Energy Bridge Gulf of Mexico LLC about 116 miles south of New Orleans, LA, in the Gulf of Mexico, is a terminal to process and transfer natural gas received from LNG transport ships to a pipeline system, which will carry the natural gas ashore for distribution to U.S. markets.** Worldwide, natural gas is in plentiful supply. However, the United States holds less than four percent of the world reserves. The Deepwater Port Act of 1974, as amended in 2002, recognized the need for new LNG import facilities and provided American industry with the option of constructing new LNG port facilities in the waters beyond the territorial limits of the United States. The new deepwater port makes it easier to import natural gas from fuel tankers, without disruption to shoreline communities and the environment.
Source: http://www.dot.gov/affairs/marad0304.htm

[Return to top]

Chemical Sector

Nothing to report.

[Return to top]

Defense Industrial Base Sector

3. *January 14, Voice of America* — **Rumsfeld resists calls for bigger U.S. Army. With over 100,000 U.S. soldiers in Iraq and another 100,000 poised to relieve them, defense officials concede the half−million strong U.S. Army, with additional missions in Afghanistan, South Korea and other points around the world, is being severely tested. That has led to new calls for a bigger army. However, Secretary of Defense Donald Rumsfeld is resisting the idea.** Speaking to reporters at the Pentagon, Rumsfeld said he is not sure an increase is in the best interests of the military or the American taxpayer. While he acknowledges the army is currently under stress, he argues it is temporary and he predicts the scope of U.S. deployments to Iraq will eventually fall off. To ease the burden on American soldiers in Iraq, Rumsfeld says a number of measures are being taken. First, more security responsibilities are being turned over to Iraqis, whose security forces are now approaching 200,000 in number. Secondly, he says the level of international military participation in Iraq is also increasing. Also, **Rumsfeld**

says the Pentagon is investing in new technologies, weapons and other equipment that will boost military capabilities. He says that is a better investment than increasing the number of soldiers in the army.
Source: http://www.voanews.com/article.cfm?objectID=888D896F−A142−43D4−826635C7FFF99BB4

[Return to top]

Banking and Finance Sector

4. *January 15, Financial Times* — **HBOS fined over US$2.2 million over money laundering rules. HBOS, the UK's fourth largest bank, was fined US$2.29 million over breaches of money laundering rules by financial regulators on Thursday, January 15.** The Financial Services Authority (FSA) said its investigation had revealed weaknesses in the record keeping systems and controls at HBOS's Bank of Scotland unit. "The failure by Bank of Scotland to keep proper records of customer identification could have seriously undermined its ability to comply with the requirements of orders served by law enforcement agencies," said Andrew Procter, the FSA's director of enforcement. **The FSA found that in over a half of accounts it sampled Bank of Scotland failed to keep a copy of the customer identification or a record of where it could be obtained. The problem was intensified by the bank's inability to determine where its record keeping had broken down.** Bank of Scotland, which alerted the FSA to the problem, issued a statement saying it accepted the fine and regretted its error. It added that it had quickly remedied the problem. "There is no evidence of any money laundering or of any Bank of Scotland customers having been adversely affected as a result of the problem," the bank said.
Source: http://news.ft.com/servlet/ContentServer?pagename=FT.com/StoryFT/FullStory&c=StoryFT&cid=1073281045049

5. *January 15, Australian Associated Press* — **Westpac warns Australian customers. Westpac Bank is warning its Internet banking customers that they are again being targeted by fraudsters hoping to gain their banking details by directing them to a bogus Website.** Westpac spokesperson Paul Gregory said the bank had discovered Thursday, January 15, that some of its customers were receiving an e−mail containing a link which took them to a fake Westpac Website. **The customers are asked to enter their details and password on the site which he says "looks pretty convincing."** He said Westpac had posted a fresh warning on its Website about the scam. Gregory said it appeared the scam was directed at Australian Westpac customers as the fake Website was for Westpac Australia.
Source: http://www.smh.com.au/articles/2004/01/15/1073877955031.html

6. *January 15, IDG News Service* — **PayPal scam spreads Mimail worm.** After releasing a new version of the Mimail e−mail worm last week, virus authors are using a new tool to help it spread −− spam e−mail containing a Trojan horse program that, once installed, retrieves and installs the worm. **The new threat, which targets customers of EBay's PayPal online payment service, highlights a growing trend in which online criminals combine computer viruses, spam distribution techniques, Trojan horse programs, and "phishing" scams to circumvent security technology and fool Internet users,** says Carole Theriault, security consultant at Sophos. Antivirus companies warned customers Thursday, January 15, about the

new threat, which arrives in e−mail in−boxes as a message purporting to come from online payment service PayPal. For their computers to be infected, users who open the compressed Zip file attached to the e−mail must then open a second file, which installs a Trojan horse program. That program connects to a Website in Russia and retrieves the latest version of the Mimail worm, Mimail−N, Theriault says. Once installed, Mimail−N alters the configuration of Microsoft Windows so that the worm is launched whenever Windows starts, harvests e−mail addresses from the computer's hard drive, and mails copies of itself out to those addresses.
Source: http://www.pcworld.com/news/article/0,aid,114340,00.asp

7. *January 14, Continuity Central* — **Telecommunications vulnerabilities pose significant threat to banking sector. A U.S. working group of banking experts is recommending that the private sector find ways to develop secure and resilient telecommunications essential for critical banking functions.** The group, known as the Working Group on Government Securities Clearance and Settlement, issued detailed recommendations to the government last week. Industry, the Federal government, and state governments have been considering the resilience of wholesale banking activities since terrorists destroyed key telecommunications infrastructure on 9/11. The attacks revealed serious operational vulnerabilities. **The Working Group first and foremost recommends that banking infrastructure owners undertake responsibility for attaining sufficient infrastructure resilience.** Fulfilling this responsibility involves "achieving geographically dispersed resources, covering equipment and systems, data, and staff," and other due diligence activities. In addition to telecommunications resilience, the Working Group is recommending renewed focus on cyber−terrorism and regulatory impediments experienced during, and in the aftermath of, a significant disruption. Finally, the report recommends support for The Bond Market Association's Emergency Subcommittee, which is examining real−time information sharing and crisis communications.
Source: http://www.ds−osac.org/view.cfm?KEY=7E455D424A5C&type=2B170C1E0A3A0F162820

[Return to top]

Transportation Sector

8. *January 15, Associated Press* — **Jet strike on Washington still slim possibility, officials say.** U.S. and Canadian military aircraft have scrambled nearly 1,700 times to intercept or divert suspicious aircraft since September 11, but routine drills illustrate how terrorists could penetrate the airspace around the nation's capital. "We do these tests to push the system, find holes, and when we find holes we correct them," said Canadian Army Maj. Douglas Martin of the North American Aerospace Defense Command (NORAD). **Officials said the exercises conducted in early− and mid−December are the latest to show that the best prevention against another terror tragedy in the skies is thorough pre−emptive intelligence and screening, not a last−minute intercept or shootdown of a hijacked commercial airliner.** They said U.S. military officials have concluded it would be very difficult to intercept a hijacked plane within a certain radius of major cities like Washington unless fighter jets were already airborne. "Since September 11, Homeland Security and the Department of Defense have vastly improved the coordination response capacity of the nation's air defenses, and we are continually exercising and training to ensure we have the right assets in place to address any threats," Homeland spokesman Brian Roehrkasse said.

Source: http://www.usatoday.com/news/washington/2004−01−15−dc−air_x. htm

9. *January 15, FOX News* — **Airports to allow two tries at detectors.** Fewer air travelers will have to take off their shoes and get their carry−on bags searched at security checkpoints under a new screening policy at airports around the country. The Transportation Security Administration is giving people who set off metal detectors on their first pass through the metal detectors a second chance, after they've removed the coins or keys they think caused the alarm. **Before, setting off the metal detector meant a secondary search, which involves removing shoes and getting wanded while screeners search carry−on luggage. Now, those who make it through the metal detectors a second time — and who haven't been flagged for extra screening — can go right on to their gate.** The change, which took effect December 27, can save time and shorten lines, Yolanda Clark, TSA spokesperson, said Thursday. When you go through secondary screening, you've lengthened the time you've spent by three minutes," Clark said.
Source: http://www.foxnews.com/story/0,2933,108551,00.html

[Return to top]

Postal and Shipping Sector

10. *January 15, Washington Post* — **Postal Service tries pay−for−performance system.** Postmaster General John E. Potter, working with Postal Service employee groups, has launched a pay system for 70,000 management employees that uses goals and performance indicators to determine the size of their annual raises. **Potter is betting the pay−for−performance system will spur most postmasters, managers, and supervisors to continually improve mail operations because they will have a chance to earn bigger raises than in the past.** Two years ago, Potter abolished a controversial bonus program, known as EVA for "economic value added," that postal officials found difficult to explain to employees and to Congress. Since taking office in 2001, Potter has tried to cut costs. **Although revenue from first−class mail remains at risk as Americans increasingly use e−mail and the Internet, the Postal Service turned a profit last year.** Potter eliminated more than 20,000 postal jobs last year and forecasts an additional reduction of 8,500 positions this quarter. Potter described the new pay system as "strictly data driven." The pay of postmasters, managers, and supervisors will hinge on how well they meet customer service goals, improve workplace safety, and control overtime and other costs that can be measured.
Source: http://www.washingtonpost.com/wp−dyn/articles/A18458−2004Jan 14.html

[Return to top]

Agriculture Sector

11. *January 15, Associated Press* — **USDA tracing suspect cattle from Canada.** When investigators went to a Alberta, Canada, the farm's records made it easy to prove the farm raised the Holstein that brought the first known case of mad cow disease into the United States. **But investigators are having far more trouble finding the scores of other animals from the farm that came into the United States with the diseased cow. Three weeks after the**

infected animal's discovery at a Mabton, WA, farm, officials have located only 20 of the 81 cows they are looking for. That is because finding each cow requires a painstaking search. "It's a paper trail. We look at import documents, health certificates, farmer sales, and shipping orders," said Jim Rogers, a spokesman for the U.S. Department of Agriculture (USDA). There are also interviews with ranchers, shippers, feedlot operators, and anyone else who may have come across the animals. And there is DNA testing on calves to determine whether they were offspring of the diseased cow. **The USDA has about 70 people tracking these cows. Locating all the cows from the Forsberg herd is key to ensuring mad cow disease does not spread to humans.** It also helps reduce the number of cows that have to be destroyed as a precaution.
Source: http://story.news.yahoo.com/news?tmpl=story&cid=541&ncid=751&e=3&u=/ap/20040115/ap_on_he_me/mad_cow_search

12. *January 15, Reuters* — **Taiwan reports less virulent strain of bird flu. Taiwan found a less virulent strain of the deadly bird flu at a chicken farm but says the case is isolated and poses no threat to people, health officials said on Thursday. The government began to slaughter on Thursday the 20,000 chickens on the farm in central Taiwan, and has quarantined and disinfected the property, said Yeh Ying, deputy director of the Animal Health Inspection Department.** "This case is different from the outbreak in Japan and South Korea. Theirs is a virulent strain, which means poultry and other birds will die quickly if they contract it," she told Reuters. The H5N2 strain of the virus was found at a farm in Changhwa County on January 5 after examining samples sent from dead chickens, said Yeh. "The case found in Taiwan is a weaker strain, which, although fatal to birds, cannot be passed to people," Yeh said, adding tests are also being conducted on chickens at neighboring farms. Yeh said officials are looking into possible sources for the infection, which could have been passed by migratory birds from South Korea or Japan or smuggled poultry products from China.
Source: http://www.reuters.com/locales/newsArticle.jsp?type=worldNews&locale=en_IN&storyID=4133276

13. *January 15, Daily Democrat (Woodland, CA)* — **Oyster harvest shut down by weather. This winter's storms have kept Northern California's oyster beds largely shut down.** Last week, on Tuesday and Wednesday, oystermen got a rare break and piled into boats for the season's richest haul out of Marin County's Tomales Bay, tens of thousands of Pacific oysters or Miyagis, Kumomotos, French belons, and Eastern oysters. **A half−inch storm locks up all but one of Tomales Bay's oyster leases for four to six days.** State and federal food safety regulations are designed to keep fecal bacteria from cattle farms and septic tanks from washing into oyster beds. Scientists found that half−inch storms were enough to flush bacteria into the bay, exceeding a standard that's less than a tenth of the concentrations that public−health officials use as a trigger to order beach closures to swimming and surfing. **For most oystermen, wintry storms every three to four days has blocked harvest for all but a single 18−hour window in mid−December and about 36 hours this week.**
Source: http://www.dailydemocrat.com/articles/2004/01/14/news/news9__.txt

14. *January 15, Associated Press* — **Cattle from brucellosis herd shipped to slaughter. About 260 cattle from a western Wyoming ranch were sent to slaughter Wednesday, the latest step in federal and state efforts to prevent spread of brucellosis.** In December, 31 cattle from the herd were diagnosed with brucellosis and were destroyed. The cattle hauled away Wednesday had tested negative but were sold off as a precaution. **Although the source of**

infection has not been pinpointed, wildlife researchers are focusing on a state elk feedground next to the infected ranch. Elk there have had brucellosis in the past. The feedgrounds were put in place to prevent elk from wandering onto cattle pastures and rangeland. **Three states, California, Colorado, and Nebraska, have placed restrictions on movement of Wyoming cattle, and other states are watching to see results of further testing.** About 3,800 cattle in eight neighboring herds have tested negative for brucellosis although four cows were labeled suspect because of conflicting results. A second round of tests will be taken in the spring. If an animal from a second herd tests positive, Wyoming would lose its federal brucellosis free status and cattle in the state would be subject to severe restrictions on movement.
Source: http://www.trib.com/AP/wire_detail.php?wire_num=53606

15. *January 14, Reuters* — **Herd under quarantine due to mad cow. Another dairy herd in Washington state was placed under quarantine after at least one animal was linked to a Holstein cow infected with mad cow disease, the U.S. Department of Agriculture (USDA) said on Wednesday.** USDA said at least one herdmate of the infected cow was sent to a dairy facility in Quincy, Washington. "USDA believes that as many as seven animals may have been sent to this facility," it said in a statement. The USDA has been investigating the nation's first case of mad cow disease, discovered on December 23 in a Holstein dairy cow in Washington.
Source: http://www.reuters.com/newsArticle.jhtml?type=scienceNews&st oryID=4127721

[Return to top]

Food Sector

16. *January 15, Agricultural Research Service* — **Safer poultry. Agricultural Research Service (ARS) scientists have found several promising intestinal bacteria that could protect live chickens from Salmonella, Campylobacter, and other pathogens that cause foodborne illness in people who eat poultry.** To prevent contamination of the meat, it's important to prevent the pathogens from taking hold inside the intestinal tracts of the live birds. ARS scientists are getting a better understanding of how live beneficial bacteria, called probiotics, influence the gut's microbial environment and interact with other bacteria. Probiotics contribute to the intestinal tract's health and balance. They are given orally to poultry to help the birds fight illness and disease. Using a concept known as competitive exclusion, probiotics are fed to newly hatched poults. Once inside, the probiotics occupy sites in the young bird's intestinal tract where the pathogens would normally attach and grow. Since probiotics get there first, they reduce the opportunity for pathogenic bacteria to become established in newly hatched poults when they are most susceptible to infection. The scientists have already screened more than four million intestinal isolates to come up with several promising probiotic combinations.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

[Return to top]

Water Sector

17.

January 15, Water Tech Online — **British water mergers may be undermined by U.S. study.** British water regulator Ofwat has released an independent study conducted by a U.S. water utility services firm that may undermine the case for any water and sewerage companies planning mergers and takeovers within the industry. **The study found there was "no evidence of general economies of scale in the water industry."** Analysts have long seen regulatory barriers to intra−sector takeovers and mergers as having a depressing effect on water share prices. The study was commissioned by Ofwat. It examined data collected by Ofwat from the industry over the past 10 years.
Source: http://www.watertechonline.com/news.asp?mode=4&N_ID=45425

[Return to top]

Public Health Sector

18. *January 15, Herald Sun − Australia* — **Bird flu spreads. Vietnam said Wednesday it had detected 18 suspected cases of bird flu in humans, and that 13 victims had died.** "Eighteen people have been found to have contracted influenza A, of whom 13 died, including 11 children and two adults," Vietnam News Agency said. The World Health Organization (WHO) has confirmed three deaths from the H5N1 virus in Vietnam, but it says it is carrying out tests to determine if bird flu killed the others. The same strain of bird flu killed six people in Hong Kong in 1997, when more than one million chickens and ducks were killed.
Source: http://www.heraldsun.news.com.au/common/story_page/0,5478,8399350%255E663,00.html

19. *January 15, Washington Times* — **Vaccines from plants. A U.S. company Wednesday, January 14, announced a four year, $5.7 million research agreement with the National Institutes of Health (NIH) to develop vaccines from genetically engineered plants. The agreement follows NIH requests for new vaccine technologies against infectious diseases, including biological weapons.** Plant−based vaccines are cheaper and easier to produce than existing vaccines, company officials said. The plant−based vaccines could be used for nearly any disease. **"This can be used in any situation in which there is a need to develop a vaccine quickly and vaccinate large numbers of people,"** said company spokesperson Adrianne Proctor. The company intends to develop vaccines from proteins produced on the leaves of greenhouse−grown plants. The proteins stimulate an immune response in the human body that blocks the development of disease. The plant systems avoid the traditional vaccine process of fermenting bacteria in sterile vats by growing the genetically engineered proteins on plants. Drug companies often spend $500 million to $700 million to build new vaccine−fermentation facilities, which can take five to seven years before they start operating. Genetically engineered plants eliminate the need for fermentation and reduce costs by about 50 percent.
Source: http://washingtontimes.com/business/20040114−094659−1049r.ht m

20. *January 15, Associated Press* — **CDC study: Flu shot doesnt fend off related illnesses. This season's flu vaccine had little effectiveness against preventing flu−like illnesses, from the common cold to even strep throat, according to the results of a federal study released Thursday.** In the study, Colorado hospital workers who received flu shots were asked whether they developed flu−like symptoms, a fever plus a cough or a sore throat. The U.S. Centers for

Disease Control and Prevention (CDC) said its preliminary data indicates the flu shot had little or no effect against those flu−like illnesses. **The data did not surprise CDC officials, who expected this seasons flu shot to only be about 30 percent effective in preventing flu−like illnesses.** "We can't draw any conclusions of the effectiveness of the vaccine against influenza−like illness," said Ed Thompson, the CDCs deputy director for public health science. The study did not say how effective this years flu vaccine was against flu virus strains, Thompson said. Other tests are being conducted to determine that.
Source: http://www.accessnorthga.com/news/ap_newfullstory.asp?ID=291 91

21. *January 15, Reuters* — **Genes make some people more prone to SARS. Scientists in Hong Kong have discovered people with a certain pattern of genes have a much higher risk of getting Severe Acute Respiratory Syndrome (SARS), a finding that could help diagnose and prevent the spread of the disease.** A study of SARS patients in Hong Kong showed individuals with a pattern known as HLA−B*0703 were four times as likely to contract the respiratory disease, said Paul Chan, an associate professor in microbiology at the Chinese University of Hong Kong. Those with a pattern labeled HLA−DRBI*0301 had a much lower risk, indicating genetic make−up may play a key role in determining if some people are more susceptible to the virus than others. "Our findings from this study will help us more accurately diagnose the disease and design effective prevention programs," Chan said. **"For example, we could test an unproven vaccine or prevention method on the high−risk group. Hospitals may also consider sending only low−risk health workers to take care of SARS patients," he said.** The Hong Kong researchers examined the blood samples of 90 SARS patients and studied the patterns of their human leucocyte antigen (HLA) genes, which influence the activity of cells that are responsible for the immune system's response.
Source: http://www.reuters.com/newsArticle.jhtml?type=healthNews&sto ryID=4131916

22. *January 14, Voice of America* — **Zimbabwe suffers anthrax outbreak. An outbreak of anthrax in Zimbabwe has killed three people and infected nearly 200 others.** Health officials are struggling to deal with the outbreak. The medical director for the southeastern Masvingo province, Tapiwa Magure, confirmed the deaths and said about 200 people have been treated for anthrax. **Magure says the health ministry has enough drugs to deal with the disease in humans, but there seems to be a shortage of vaccines for cattle to contain the outbreak.** He said the veterinary service has launched a vaccination program in the affected area. But he said they can only do so much with the available resources. Anthrax most commonly occurs in wild and domestic animals such as cattle, sheep, and goats. Humans can be infected by handling meat and other products from infected animals. Anthrax can also spread if people eat undercooked meat from an infected animal.
Source: http://www.voanews.com/article.cfm?objectID=6AFADF18−1718−46 70−8D68CFDAD2B3A830

[Return to top]

Government Sector

Nothing to report.

[Return to top]

Emergency Services Sector

23. *January 15, NOAA News* — **NOAA satellites prove critical in fishermen rescue.** Three shrimp fishermen were pulled to safety Wednesday, January 14, after their boat sank 15 miles east of Port Isabel, TX. **The fishermen used an emergency beacon to send out a distress signal, which was picked up by NOAA (National Oceanic and Atmospheric Administration) satellites, and relayed to the agency's Mission Control Center in Suitland, MD.** The staff at the center verified the signal, which came from an Emergency Positioning Indicating Radio Beacon or EPIRB, pinpointed the location of the fishermen's boat Dona Nelly, and notified the U.S. Coast Guard, which carried out the rescue. The rescue operation was engineered by the international Search and Rescue Satellite−Aided Tracking System (COSPAS−SARSAT). Since SARSAT became operational in 1982, almost 17,000 lives have been saved worldwide, including more than 4,600 in the United States. "The SARSAT system helped prevent an unfortunate mishap from becoming a deadly tragedy," said Ajay Mehta, the NOAA SARSAT program manager. The NOAA Satellites and Information Service is the nation’s primary source of space−based meteorological and climate data. It operates the nation’s environmental satellites, which are used for weather and ocean observation and forecasting and climate monitoring.
Source: http://www.noaanews.noaa.gov/stories2004/s2155.htm

24. *January 15, Daily Nexus (Santa Barbara, CA)* — **Robot clears lab of explosive acid.** The Santa Barbara County, CA, Bomb Squad, Hazardous Materials Unit and Fire Dept. responded to a potentially explosive situation on Tuesday afternoon, January 13, when two jars filled with a material believed to be crystallized picric acid were found. **The jars were discovered in a pathology lab on the 300 block of Patterson Avenue. Picric acid, a derivative of phenol, becomes sensitive to explosion when it reacts with metal and can be easily detonated by heat, flame, shock or friction.** Approximately 50 people were evacuated and the bomb squad used **a remote−controlled robot to enter the laboratory and bring the containers down the elevator and out of the building.** "They sent the robot in there and used cameras to maneuver the robot," Fire Dept. Capt. Charlie Johnson said. "The containers were placed in a trash can filled with dirt and were taken down the elevator to a bomb trailer. The operators were in the parking lot several feet away." The containers were put in a bomb trailer −− a cylindrical device designed to explode upward instead of outward −− and transported to the Tajiguas landfill for detonation. **"They kept everybody back at a safe distance until they got to the landfill site," Johnson said. "A significant explosion occurred, and it most probably was picric acid in crystallized form."** No one was hurt in the incident.
Source: http://www.ucsbdailynexus.com/news/2004/6365.html

25. *January 14, Global Security Newswire* — **Agency helps Greece defend against Olympic 'dirty bomb' attack.** With the threat of terrorism looming over this year's Summer Olympics in Athens, the United States is helping Greece to deploy radiation detectors in a bid to prevent a radiological attack on the summer games. **The National Nuclear Security Administration (NNSA) and Greece are installing fixed radiation detectors at seven locations, focusing on border crossings, NNSA Administrator Linton Brooks told reporters Tuesday, January 13.** Portable detectors will be used at other locations. Brooks said the detectors are similar to those used in the Energy Department's Second Line of Defense Program, designed to help Russia and other key countries detect trafficked nuclear material. After Greece asked the

International Atomic Energy Agency for help in heading off a potential "dirty bomb" attack, the UN agency in turn requested U.S. assistance with the project. Besides installing detectors, NNSA is giving the IAEA $500,000 for equipment to be used at Olympic venues. NNSA is training Greek personnel to use and maintain the detection equipment, and is securing several sealed radiological sources in Greece.
Source: http://www.govexec.com/dailyfed/0104/011404gsn1.htm

[Return to top]

Information and Telecommunications Sector

26. *January 15, Government Accounting Office* — **GAO−04−157: Status of Federal Public Key Infrastructure Activities at Major Federal Departments and Agencies (Report).** The federal government is increasingly using online applications to provide access to information and services, and to conduct internal business operations. As such, **strong security assurances are necessary to properly safeguard data. The Government Accounting Office (GAO) found that Public Key Infrastructure (PKI) and its associated hardware, software, policies, and people can provide greater security assurances than simpler means of authenticating identity, such as passwords**. Twenty of the 24 agencies reported that they are undertaking a total of 89 PKI initiatives, now in various stages of development. Agencies continue to face challenges, however, in PKI implementation, many of which are similar to those faced in GAO's 2001 report on the issue. Policy and guidance is often lacking or ill−defined, including in technical standards and legal issues. Insufficient funding for the high cost of PKI technology also is a challenge. Interoperability continues to be an issue, as integrating PKI with other systems at times requires significant change or even replacement. Another challenge is the administrative burden of training personnel for use and management of PKI.
Source: http://www.gao.gov/highlights/d04157high.pdf

27. *January 15, CNET News* — **Agriculture epidemics may hold clues to Net viruses. In studying the effects of last summer's MSBlast worm, some security experts turned to an unlikely source in search of clues to the prevention of computer epidemics: plants. Their idea was inspired by parallels that scientists are drawing between the proliferation of computer viruses and the spread of agricultural catastrophes** such as Dutch Elm Disease, which has devastated a small variety of American elms since crossing the Atlantic decades ago. Like Dutch Elm, MSBlast was a single foreign entity that infected extremely susceptible hosts of an entire population−−in this case, of Windows computers. "People have brought over species that we didn't expect here, just like people have created viruses that Microsoft didn't expect to deal with," said Jeff Dukes, professor of biology at the University of Massachusetts at Boston, who studies diversity and growth in ecological systems. **Computer security experts see similarities between the way a disease can devastate agricultural crops and the way a virus can attack Internet infrastructure. The reliance on one type of technology, software or protocol has created digital "monocultures," a phrase borrowed from botany that refers to ecosystems vulnerable to disastrous harm from a single disease**.
Source: http://news.com.com/2009−7349_3−5140971.html?tag=nefd_lede

28.

January 14, CNET News — **Browser security takes off in VPNs. Corporations are embracing a simpler, cheaper way of connecting remote workers to their networks −− Secure Sockets Layer (SSL) encryption. SSL is a significant step forward in Virtual Private Network (VPN) ease−of−use as an alternative to Internet Protocol security (IPSec)**. SSL technology has been embedded in most standard Web browsers for years. **SSL VPNs enable access from virtually any Web browser, so they're a natural fit for remote access and extranet applications**. For most Web−based applications, users don't have to use a client, making it easier to give access to the network. IPSec VPNs require the installation and configuration of software on all clients and can be clunky when it comes to remote access, often meaning interoperability issues that can leave many frustrated and stranded without access to critical network information. Most experts agree that the technologies are complementary. Though SSL VPN has many benefits, it also has its downside. One important element is end−point security. SSL VPN allows people to enter corporate networks via any Web browser, socompanies need to make sure that it has strong authentication to verify that users are authorized. It also needs strong policy management to ensure that people only access applications for which they have approval. As people can use any Web−enabled device for access, viruses from those machines can be transmitted to the corporate network.
Source: http://news.com.com/2100−1033_3−5140548.html

29. *January 14, Federal Computer Week* — **Commerce to fund IT security. A senior Commerce Department official said funding will be poured into information technology security this year.** Michael Sade, director for acquisition management and procurement executive, said the real impact of IT security isn't going to be on the technology side, but on the personnel side −− such as ensuring vendors have security clearances. Sade generally spoke about how Commerce officials will better partner on projects with vendors and other government agencies through dialogue. **Significant projects underway include modernization of the Patent and Trademark Office and National Weather Service. Commerce has begun making significant IT investment in preparation for the 2010 Census −− possibly including the capability of doing surveys through the Web,** Sade said. Another growing trend will entail better review of satellite programs in which the department funds projects that are overseen by other departments and agencies.
Source: http://www.fcw.com/fcw/articles/2004/0112/web−sade−01−14−04. asp

Internet Alert Dashboard

Current Alert Levels

 AlertCon: 1 out of 4 https://gtoc.iss.net	 Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	

	#1 Virus in the United States: **PE_PARITE.A** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	135 (epmap), 1434 (ms−sql−m), 137 (netbios−ns), 445 (microsoft−ds), 17300 (Kuang2TheVirus), 6129 (dameware), 80 (www), 139 (netbios−ssn), 53 (domain), 3410 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

30. *January 15, Associated Press* — **Libya ratifies nuclear test ban treaty. In a new signal that Libya is serious about renouncing its weapons of mass destruction, UN officials said Wednesday the North African country has ratified the nuclear test ban treaty.** Libya's nuclear program was far from producing a weapon and the treaty is 12 nations short of the 44 ratifications needed for it to enter into force. Still, the announcement by the UN agency overseeing the agreement appeared to be a further sign of commitment by Libyan leader Moammar Gadhafi to give up nuclear weapons ambitions. The UN agency, known as the Preparatory Commission for the Comprehensive Nuclear Test Ban Organization, said that in ratifying the pact earlier this month, Libya agreed to host a monitoring station at Misratah. That would be part of a network of 337 stations being set up worldwide to verify compliance with terms of the treaty. Libya announced December 19 it was giving up its weapons of mass destruction after months of talks with the U.S. and Britain. Since then, both the International Atomic Energy Agency, the UN nuclear watchdog, and the U.S. have sent experts to Libya to take inventory of Libya's nuclear activities ahead of supervising their destruction.
Source: http://story.news.yahoo.com/news?tmpl=story&cid=515&ncid=721&e=9&u=/ap/20040114/ap_on_re_af/libya_nuclear

31. *January 15, Cox News Services* — **U.S. forces capture No. 54 on Iraqi list.** U.S. military officials announced Wednesday that they had captured another of the top 55 fugitives from Saddam Hussein's regime, reducing its list of those at large to 13. **Khamis Sirhan al−Muhammad, suspected of involvement with ongoing insurgent attacks and No. 54 on the U.S. list, was taken into custody Sunday near Ramadi in an operation by Special Operations forces and members of the 82nd Airborne Division, Brig. Gen. Mark Kimmitt told reporters.** "With the capture of No. 54, we have taken another significant step in reducing anti−coalition resistance," Kimmitt said in Baghdad. "He was an enabler for many of the resistance attacks on Iraqis as well as U.S. and coalition forces." Al−Muhammad's capture reduces to 13 the number of the 55 that the U.S. military does not consider captured, killed, or having surrendered. According to Central Command's list, only two of the most wanted have been killed: Saddam's sons, who were shot during a firefight with U.S. troops in July. Three of the 55 are listed as having surrendered. The rest were taken into custody, many by U.S. troops searching for Saddam and his supporters.
Source: http://www.canoe.ca/NewsStand/WinnipegSun/News/2004/01/15/31 3363.html

32. *January 15, Reuters* — **China, Russia, Central Asians open security office. China, Russia, and four Central Asian states opened a regional security headquarters on Thursday, trying to breathe life into an anti−terror forum critics say has little to show for itself after**

seven years of existence. Foreign ministers from the six countries hailed the launch in Beijing, China, of the administrative office of the Shanghai Cooperation Organization (SCO) China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan. **Secretary−general Zhang Deguang said the group aimed to intensify anti−terror efforts and discuss ways to fight drug trafficking, which he said finances regional terrorism.** The SCO, born as the Shanghai Five in 1996 to resolve Soviet−era border disputes, admitted Uzbekistan in 2001 and shifted its focus to combating Islamic militants. Analysts say the group has taken a long time to find its feet and its few successes have been small. Zhang said the SCO would be operating on a shoestring budget of $3.5 million in 2004. He said Russia and China would each foot 24 percent of the bill. Kazakh Foreign Minister Kasymzhomart Tokayev said the member states should set up and improve a system for travel and transport, a "very important responsibility." He also said the group needed to hammer out agreements on how to handle emergencies such as natural disasters.
Source: http://www.reuters.com/locales/newsArticle.jsp;:4006a652:44cca8607b34d1e?type=worldNews&locale=en_IN&storyID=4133467

33. *January 15, Associated Press* — **Saudi authorities discover militants' camps.** Saudi authorities have discovered a number of camps outside Saudi cities used for training al Qaeda militants to carry out terror operations, an Interior Ministry official said Thursday. **Two militant figures killed in terror sweeps last year −− Turki Nasser al−Dandani and Yosif Salih Fahd Ala'yeeri −− commanded the camps, the official told The Associated Press.** Saudi authorities had previously acknowledged that there may be al Qaeda training facilities in the kingdom. In July, Interior Minister Prince Nayef said most of the Muslim militants arrested or killed in a government crackdown were trained in al Qaeda camps in Afghanistan, but said "a small number perhaps were trained on farms and the like inside the country." The desert camps were set up to train militants to use weapons and self−defense techniques and also prepare them for terror operations, the official said. He did not specify the number of camps that were discovered.
Source: http://www.usatoday.com/news/world/2004−01−15−terror−camps_x .htm

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.